Example:

Migration of Existing Federal Identity Card Programs

to the

FIPS 201 Personal Identity Verification Card Specification

White Paper

Prepared for the National Institute of Standards and Technology

Revision Date: November 5, 2004
Version: 1.2
Status: DRAFT
Author: Scott Guthery, Mobile-Mind, Inc.
Point of Contact: Jim Dray, NIST

Table of Contents

Executive Summary

Federal Government smart card programs have been moving toward the Government Smart Card Interoperability Specification, Version 2.1 (published as NISTIR 6887, 2003 Edition). The Department of Defense Common Access Card program is one example of a large scale card deployment that is in the process of becoming GSC-ISv2.1 compliant.

Homeland Security Presidential Directive 12 mandates a federal employee identity verification framework that operates across agency boundaries. The National Institute of Standards and Technology is tasked to develop a standard for this framework. This standard, currently known as FIPS 201, will be based on the existing GSC-IS work, but will require an evolution of the GSC architecture to meet the requirements of HSPD-12 and to further align with existing smart card standards. The FIPS 201 integrated circuit card platform must be:

- Compliant with existing standards to the greatest possible extent
- Technology neutral, i.e. support both Virtual Machine and file system cards
- Easily implementable on low end card platforms
- Inclusive of standardized card management
- Achievable from the current GSC-ISv2.1 baseline

All integrated circuit cards in today's GSC-ISv2.1 and CAC card programs are either FIPS 201 compliant or can be field upgraded to comply with FIPS 201. In particular, CACv2 cards using GlobalPlatform 2.0.1 for card management and the three GSC-ISv2 card applications are FIPS 201 compliant.

All software – application software, client software, middleware and card management software – in today's GSC-ISv2.1 and CAC card programs can work unchanged with some FIPS 201 compliant cards. If this software does not include support for GSC-ISv2.1 file system cards then it is not GSC-ISv2.1 compliant and will have to brought into FIPS 201 compliance by adding file system support.

Today’s GSC-ISv2.1 integrated circuit cards (both Virtual Machine and file system) can be updated to comply with FIPS 201. The same is true for GSC-ISv2.1 middleware and client application programs. The semantics of the GSC framework have been preserved, and the migration to FIPS 201 primarily involves syntactic changes to the interfaces defined in GSC-ISv2.1. This report provides strategies for migration from GSC-ISv2.1 and CAC to FIPS 201. It provides a variety options from which card program managers can construct migration plans, roadmaps and timelines.

- THIS REPORT IS NOT PRESCRIPTIVE -

Background

The preliminary draft of FIPS 201– FIPS PUB 201, Federal Personal Identity Verification (PIV) Standard, Preliminary Draft, Version 1.0, October 20, 2004 – includes an accompanying Special Publication(SP 800-73) containing a definition of a general-purpose integrated circuit card for use by U.S. federal agencies in personal identity verification and access control systems. For the purposes of this document, the term "FIPS 201" will refer to the integrated circuit card specification unless otherwise noted.

As interoperability between personal identity verification systems deployed by disparate federal agencies is a key goal of standard, SP 800-73 describes the integrated circuit card in sufficient technical detail so that independent implementations are interchangeable.

To achieve this goal, the standard draws on in-depth knowledge of existing integrated circuit card standards and takes advantage of experience gained in the U.S Department of Defense Common Access Card program and programs based on the Government Smart Card Interoperability Specification.

The specification provides sufficient technical details that independent implementations are interchangeable and interoperability across federal personal identity verification and access control systems is technically achievable.

The integrated circuit card defined by the specification:

- meets the operational and security requirements of federal agencies
- is economical to produce and manage
- carries forward interoperability in existing card programs

In the process of taking advantage of existing experience and practice, the FIPS 201 integrated circuit card specification has adopted features of existing cards such as post-issuance application loading that have proven to be of value. The specification has also harmonized features of existing cards, particularly in the area of card management and administration, which first-hand experience had shown needed to interoperate more smoothly.

Purpose and Scope

The purpose of this report is to describe in detail how the federal card programs that have contributed to the definition of the FIPS 201 integrated circuit card can migrate to the use of this card and thus participate in the value to flow from the use of the card as outlined above.

The report focuses on card programs based on the NIST GSC-ISv2.1 specification such as the Department of Defense Common Access Card specification but the migration strategies proposed are generally applicable to any existing federal card program.

Overview of FIPS 201 Migration Strategies

FIPS 201 builds on the distinction between card management and card applications that was introduced in GSC-ISv2.1. A FIPS 201 integrated circuit card is a card platform on which card applications are loaded.

The primary purpose of FIPS 201 is to provide a detailed technical specification for loading application code and application data onto the FIPS 201 platform and for administering of application code and application data during their lifecycles.

A secondary purpose of FIPS 201 is to provide a detailed technical specification for the applications that were defined in GSC-ISv2.1.

Categorization of Migration Strategies

With this background, FIPS 201 migration strategies can be categorized according to the properties of the card management, card application and card data model aspects of the existing card program.

- Card programs that use GP2.0.1 for application loading and that load the card with the GSC-ISv2.1 applications are application-compliant with FIPS 201.

- Card programs that use the file system specification of GSC-ISv2.1 for data model storage, access and management can update the GSC-ISv2.1 card capability container and become data-model-compliant with FIPS 201.

- Card programs that use card management protocols other than GP2.0.1 but load the GSC-ISv2.1 applications can either update those protocols to those defined by FIPS 201 or move their applications to a FIPS 201 platform.

- Card programs that use card management protocols in GP2.0.1 but load applications that provide the functionality of the GSC-ISv2.1 applications can update these applications to be GSC-ISv2.1 compliant or they can load GSC-ISv2.1 applications onto the cards.

- Card programs that use card management protocols other than those provided by GP2.0.1 and load applications that provide the functionality of the GSC-ISv2.1 applications can update these applications to be GSC-ISv2.1 compliant and move them to a FIPS 201 platform or can load GSC-ISv2.1 applications onto a FIPS 201 platform.

It is not known how many card programs or how many cards are in each of these categories.

This general categorization of FIPS 201 migration is summarized in Table 1 below.

Migration of Federal Card Programs to		*Card Applications*		*Card Data Model*	
		GSC-ISv2.1	*Other*	*GSC-ISv2.1*	*None*
Card Management	*GP 2.0.1*	No application migration necessary	Load GSC-ISv2.1 applications on existing cards	Modify CCC to map to FIPS 201 card platform commands	Add support for FIPS 201 card platform commands
	Other	Switch to GP 2.0.1 or move applications to FIPS 201 card	Upgrade applications and move them to a FIPS 201 card	Modify CCC and switch to GP2.0.1 card management	Add support for FIPS 201 card platform commands and switch to GP2.0.1 card management

Table 1: Migration Strategies for Today's Federal Card Programs

Migration Strategy by System Component

The migration to FIPS 201 will be considered for the following components of existing federal smart card programs based on GSC-ISv2.1 and the Common Access Card specifications:

- *BSI application programs* written against the GSC-ISv2.1 and Common Access Card Basic Service Interfaces
- *BSI middleware* that implements the above GSC-ISv2.1 and Common Access Card application programming interfaces
- *card management software*, primarily card administration and management middleware, written directly against the card edge of GSC-ISv2.1 and Common Access cards
- *integrated circuit cards*, primarily GSC-ISv2.1 cards and Common Access Cards

BSI Application Programs

The conceptual model of a federal integrated circuit card surfaced on the GSC-ISv2.1 and Common Access Card Basic Service Interfaces is unchanged by FIPS 201. FIPS 201

does call for some changes in the details of the entry points defined in these two existing programming interfaces and extends these two programming interfaces to card management functionality.

The changes in the existing programming interfaces suggested in FIPS 201 unify and simplify these two variants of the Basic Service Interface. They also take into account suggestions from BSI application programmers – for example those in the DMDC API document and those coming out of the BSI reference implementation work – on the manner in which card services are represented and accessed on these application programming interfaces.

The impact on existing CAC and GSC-ISv2.1 applications written against these two existing BSI definitions will be the need to make a syntactic editing pass to change entry point signatures.

Migration Strategy for BSI Application Programs

The migration strategy proposed below for the software that implements the BSI and FIPS 201 application programming interfaces, the BSI middleware, calls for this software to support interworking of existing and new cards. The result is that existing BSI application programs can use existing GSC-ISv2.1 and CAC cards as well as FIPS 201 compliant cards without being aware of which card is being accessed.

Included in this migration strategy are higher-level application programming interfaces written on top of the BSI such as middleware that creates the DMDC Common Access Card Application Programming Interface. From the point of view of this migration study, this software is subject to the same migration considerations as BSI applications noted above. But because the conceptual model of the FIPS 201 programming interface is the same as the conceptual models on the CAC and GSC-ISv2.1 programming interfaces and because the all the functionality on these interfaces is found on the FIPS 201 interface, any programs written against such higher-level programming interfaces with a high likelihood will continue to operate satisfactorily without change.

BSI Middleware

BSI middleware, software that implements the Basic Service Interface and provides its services to BSI application programs, is impacted by both the changes to the BSI and to the card edge since this software is essentially nothing more than a mapping between the two.

As noted above, all the card-in-use functionality found on the CAC and GSC-ISv2.1 basic application programming interfaces BSI is also present on the FIPS 201 application programming interfaces. Adapting the top of BSI middleware, the interface to the application programs themselves, to the FIPS 201 application programming interface will be straight-forward. The details of this change are the same as the details for BSI application programs and are provided below.

Adapting the bottom of BSI middleware, the interface to the card, could be more difficult depending on the architecture and modularization of the middleware and how tightly bound it is to particular cards. It is difficult to make general impact statements here because impact will vary by software design and this in turn varies from implementation to implementation.

The fact that GSC-ISv2.1 does not define a hard card edge has, however, led to variation across middleware implementations and a potential lack of interoperability in this area that will continue to expand as more GSC-ISv2.1 systems are deployed.

Migration Strategy for BSI Middleware

The migration strategy proposed above for BSI middleware is to support seamless access to all existing GSC-ISv2.1 and CAC cards and to the FIPS 201 card. As will be discussed below, the commands on the FIPS 201 card edge are semantically the same – and in some case syntactically the same – as the corresponding command on the CAC and GSC-ISv2.1 card edge. The result is that expanding BSI middleware to handle the differences that do exist and to conceal these differences from BSI applications is well-defined software project with little technical risk.

As the functionality of these cards is essentially identical, this is not as challenging as it might seem at first blush. Details on the method of doing this are provided below.

The fact that the FIPS 201 card does not carry a card capabilities container means that interfacing to the FIPS 201 card is in fact easier than interfacing to existing cards because no command translation needs to be considered.

Given that access to CAC, GSC-ISv2.1 and FIPS 201 cards is supported, BSI middleware can continue to surface existing BSI specifications such as the CAC and GSC-ISv2.1 specifications or the FIPS 201 application programming interface or both. New card programs deploying only FIPS 201 card that do not need to interoperate with today's CAC cards can consider using FIPS 201 only BSI middleware.

Card Management Software

Like BSI middleware, card management software interfaces directly to the card edge. This is, however, its only interface to components described in FIPS 201 and thus card management software is impacted only by the FIPS 201 card edge description.

With respect to card use, all the functionality of the card-edge commands defined by the GSC-ISv2.1 and CAC specifications is provided by the card edge commands defined by FIPS 201 and, except in a small number of cases described below, provided with the same card edge command. The main changes in the card use commands are the elimination of the card capability container and the alignment of tag-length-value data structures with common industry and international standards-defined usage.

On the other hand, with respect to card management, neither the GSC-ISv2.1 nor the CAC specifications provided sufficiently detailed technical descriptions of the integrated circuit card commands for card management to achieve interoperability among card management systems and card management software. This is a shortcoming that is explicitly addressed by FIPS 201.

The difficulty of migrating proprietary card management software to the FIPS 201 card management commands depends, of course on the architecture of that software and how deeply its proprietary commands are embedded in it.

FIPS 201 card management commands are the card management commands specified in GlobalPlatform 2.0.1.

Migration Strategy for Card Management Software

As with BSI middleware, the migration strategy proposed for card management software is to add support for FIPS 201 card administration and application management commands, including secure messaging, to existing card management software where this support is currently missing or non-compliant.

As the FIPS 201card administration and application management commands come directly from GlobalPlatform and as it is unlikely that anything other than variants of these commands are used in proprietary card management systems for GSC-ISv2.1 and CAC cards, adding FIPS 201 compliant commands should not be difficult since they are cosmetic and syntactic variants of commands already supported in the systems.

Adding secure messaging to existing virtual machine cards such as the CACv1 and CACv2 cards can be handled in transition by using a secure messaging applet when secure messaging is necessary. Existing GSC-ISv2.1 file system cards – if there are any – face a more difficult migration here because secure message handling is typically built into the smart card operating system. Nevertheless, most card vendors support some form of post-issuance operating system patches so in the extreme this approach could be taken to upgrade GSC-ISv2.1 file system cards to FIPS 201.

Integrated Circuit Cards

Migration Strategy for Integrated Circuit Cards

All of the integrated circuit cards in today's GSC-ISv2.1 and CAC card programs are either Java Cards or file system cards with a card capability container. All of these existing cards can be updated to comply with FIPS 201.

Java Cards can be brought into functional and operational compliance with FIPS 201 by adding a FIPS 201 applet. File system cards with a card capability container can be

brought into functional and operational compliance by adding FIPS 201 command translation instructions to the card capabilities container file.

Migration Overview Summary

In a nutshell, an existing GSC-ISv2.1 or CAC card program can either migrate its middleware or migrate its cards.

In the case that it is not practical to update existing GSC-ISv2.1 or CAC cards to FIPS 201 compliance, the proposed migration strategies for BSI application programs, BSI middleware and card management software, insure that existing GSC-ISv2.1 and CAC cards can interwork in the same card program and card system with new FIPS 201 cards.

In either case, since the FIPS 201 specification interworks with both GSC-ISv2.1 and CAC card specifications, the pace of the migration is driven by policy and management considerations rather than technical considerations.

The migration strategies described herein are both gradual and evolutionary. They assume operational card systems with a mixture of both cards and middleware.

Details of the Migration Strategies

As described in the previous section, there are two interfaces on which migration must be analyzed in detail: the application programming interface and the card edge.

Table 1 summarizes which migration strategies are of concern to the providers of which component. Only the providers of software tools implementing the application programming interface need be concerned with both application programming interface and card edge migration.

Component	**API Migration Strategies**	**Card Edge Migration Strategies**
BSI Application Programs	√	
BSI Middleware	√	√
Card Management Software		√
Integrated Circuit Cards		√

Table 1: Impact of Change on Card Program Software

Migration of the Application Programming Interface

The primary difference between the FIPS 201 application programming interface and GSC-ISv2.1 and CAC application programming interfaces is that FIPS 201 API supports both card use and card management applications whereas the GSC-ISv2.1 and CAC APIs support only card use applications.

With respect to card use applications, functionality of entry points on the GSC-ISv2.1 and CAC APIs is all found – often with only a syntactic difference – in the functionality of the entry points on the FIPS 201 API. Overall the functionality on the FIPS 201 card API is a subset of the functionality on the GSC-ISv2.1 API and virtually identical to the functionality on the CAC API.

The syntax and data formatting on the FIPS 201 application programming interface is in some cases different than the syntax and data formatting of the corresponding data on the GSC-ISv2.1 and CAC application programming interfaces. These details are discussed below and a migration strategy for dealing with these differences provided.

Because neither the GSC-ISv2.1 nor the CAC application programming interfaces support card management applications, there is neither portability nor interoperability of card management applications today. This has led to increased testing and acceptance costs and in some cases incompatible and non-interoperating card use behavior. FIPS 201 addresses this shortcoming of the GSC-ISv2.1 and CAC application programming interfaces by defining an API for card management as well as card use.

API Entry Points for Card Use Applications

The entry points on the FIPS 201 application programming interface are with one exception all found on the GSC-ISv2.1 and CAC application programming interfaces. The FIPS 201 application programming interface is a subset of the GSC-ISv2.1 and CAC application programming interfaces. Both the functionality and the semantics of the GSC-ISv2.1 and CAC application programming interfaces is preserved in FIPS 201.

The change in the application programming interface found in FIPS 201 vis-à-vis the GSC-ISv2.1 and CAC application programming interfaces is in the formatting of the data sent into and received back from the interface by the application program.

Tables 2-4 below list the entry points on the FIPS 201, GSC-ISv2.1 Basic Services Interface and the ActivCard Common Access Card BSI API that are used to access a card in use.

FIPS 201 Draft	*GSC-ISv2.1 Basic Services Interface*	*ActivCard Common Access Card BSI API*
Acquire Context	gscBsiUtilAcquireContext	gscBsiUtilAcquireContext
Connect	gscBsiUtilConnect	gscBsiUtilConnect
Disconnect	gscBsiUtilDisconnect	gscBsiUtilDisconnect
	gscBsiBeginTransaction	
	gscBsiUtilEndTransaction	
	gscBsiUtilGetVersion	gscBsiUtilGetVersion

	gscBsiUtilGetCardProperties	gscBsiUtilGetCardProperties
	gscBsiUtilGetCardStatus	
	gscBsiUtilGetExtendedErrorText	
	gscBsiUtilGetReaderList	
Establish Secure Channel	gscBsiUtilPassthru	gscBsiUtilPassthru
Release Context	gscBsiUtilReleaseContext	gscBsiUtilReleaseContext

Table 2: API Entry Points for Card Communication

FIPS 201 Draft	*GSC-ISv2.1*	*ActivCard Common Access Card BSI API*
Create Data Element	gscBsiGcDataCreate	gscBsiGcDataCreate
Delete Data Element	gscBsiGcDataDelete	gscBsiGcDataDelete
Get Data Element Properties	gscBsiGcGetContainerProperties	gscBsiGcGetContainerProperties
	gscBsiGcReadTagList	gscBsiGcReadTagList
Read Data	gscBsiGcReadValue	gscBsiGcReadValue
Write Data	gscBsiGcUpdateValue	gscBsiGcUpdateValue
Select Data Element		

Table 3: API Entry Points for Data Access

FIPS 201 Draft	*GSC-ISv2.1*	*ActivCard Common Access Card BSI API*
Get Challenge	gscBsiGetChallenge	gscBsiGetChallenge
Authenticate Card	gscBsiSkiInternalAuthenticate	gscBsiSkiInternalAuthenticate
Create Digital Signature	gscBsiPkiCompute	gscBsiPkiCompute
Get Certificate	gscBsiPkiGetCertificate	gscBsiPkiGetCertificate
	gscBsiGetCryptoProperties	gscBsiGetCryptoProperties
		gscBsiGetPkiProperties

Table 4: API Entry Points for Cryptographic Services

API Entry Points for Card Management Applications

Table 5 below list the entry points on the FIPS 201 application programming interface used for card management. As noted above, GSC-ISv2.1 does not define an API for card management. The result is that the application programming interfaces used today to manage both GSC-ISv2.1 and CAC cards are proprietary and the card management programs written against these interfaces are neither portable nor interoperable.

In theory card management programs written against these proprietary card management interfaces create cards that are both interoperable in use and are able to be administered by systems other than the system that created them. Practice has fallen somewhat short of theory, particularly in the area of performing card administration functions on a card that was produced by a system other than the system performing these functions.

By defining a standard card management programming interface based on the GlobalPlatform card management specification, FIPS 201 extends interoperability of federal integrated circuit cards to card management as well as card use.

FIPS 201 Draft	*GSC-ISv2.1*	*CAC*
Add Card Application	N/A	Proprietary
Delete Card Application	N/A	Proprietary
Generate Key Pair	N/A	Proprietary
Import Key	N/A	Proprietary
Get Card Application Properties	N/A	Proprietary

Table 5: API Entry Points for Card Management

Migration Strategy for Data Representation

As noted above, an area in which the FIPS 201 application programming interface differs from the GSC-ISv2.1and CAC application programming interfaces is in the formatting of data that crosses the interface; both the data that the application passes to the application programming interface and the data that it receives from the application programming interface.

The primary difference is in handling a fundamental integrated circuit card data structure called a tag-length-value data element. A tag-length-value or simply TLV data element consists of a sequence of bytes. The initial bytes contain a tag which is an encoding of the type of data contained in the TLV data structure. The next bytes in sequence are interpreted as an unsigned integer that counts the number of bytes in the final portion of the sequence that is the actual data in the TLV.

The GSC-ISv2.1 application programming interface surfaces the basic TLV data structure in two different ways depending on whether the data is being retrieved from file or an ISO-compliant application or being retrieved from a non-ISO compliant application. TLV data coming from files and ISO-compliant is surfaced in the form specified by the standard that defines TLVs. TLV data coming from non-ISO compliant applications such as the applications described in GSC-ISv2.1 is surfaced in a non-compliant form.

Since application programs written against the BSI, BSI middleware and card management software are concerned solely with the information in the TLV and not with the manner in which it is stored on the card, this difference causes useless duplication of code in all host-side software.

FIPS 201 provides a uniform representation for the TLV data structure on the application programming interface that is independent of the manner in which the data is stored on the card. This enables the card issuer and the card application program provider to change the manner in which the data is stored – computing a value on the fly, for example, rather than storing it in a file – without impacting applications using the data.

FIPS 201 represents TLV data structures on the application programming interface in the manner found in virtually all integrated circuit card standards and specifications, namely as described above as a codified sequence of bytes.

The migration strategy to unify the representation of the TLV data structure is to have the BSI middleware map the non-standard T-buffer/V-buffer representation presented at the card edge by the GSC-ISv2.1 application to the byte-sequence representation found in all other integrated circuit card systems.

This preserves the GSC-IS v2.1 applications that present non-ISO TLVs at the card edge while at the same time providing the auxiliary advantage of providing card applications with a uniform view of TLV data.

Migration Strategy for Access Control Rules

Table 6 lists the access control rules as seen on the application programming interfaces described in the GSC-ISv2.1 and CAC specifications and in FIPS 201.

FIPS 201	*GSC-ISv2.1*	*ActivCard Common Access Card BSI API*
Always	Always	Always
Never	Never	Never
PIN	PIN Protected	PIN Protected
External Authenticate	External Authenticate	External Authenticate
	External Authenticate then PIN	External Authenticate then PIN
External Authenticate or PIN	External Authenticate or PIN	External Authenticate or PIN
	Secure Channel – GP	Secure Channel – GP
		Secure Channel – DIN
Secure Channel - ISO	Secure Channel - ISO	Secure Channel - ISO
	PIN Always	
	PIN then External Authenticate	
	Update Once	
Biometric Authentication		

Zero Knowledge Authentication		

Table 6: Access Control Rules on the API

The GSC-ISv2.1 and CAC applications provide only fixed set of access control rule for the data they contain. This means that as new security policies are developed; e.g. PIN or biometric; all GSC-ISv2.1 and CAC applications and all the GSC-ISv2.1 and CAC middleware and all the GSC-ISv2.1 card applications will have to be updated to include these new conditions. Providing a process to extend this fixed list and coordinating additions to this list will become increasingly expensive and time-consuming.

Recognizing that security officers must be given the maximum amount of flexibility in describing and representing security policies, FIPS 201 follows ISO/IEC 7816-4 and defines access control rules as arbitrary Boolean expressions of the basic security conditions. Thus to a security officer can, for example, specify the access condition PIN or biometric without having to have a fixed list of access conditions extended. This approach is used, for example, in the 1.2 billion GSM/3G SIM cards used in mobile networks where network operators need express and update the security policies protecting the data on the SIM card.

The access control rules that are not included in FIPS 201 are the time-dependent ones, such as XAUTH_THEN_PIN. It is not clear how often these time-dependent access control rules are used in existing systems. Because there are details of the semantics of these rules missing from GSC-ISv2.1, it is unlikely that if they are used the usage is interoperable across application software. These time-dependent access control rules can be implemented on a FIPS 201 card using non-time-dependent access control rules on key material files should it prove necessary.

The migration strategy for access control rules is to use a common set of rules for all data resident on the card, whether computed by application or in stored in a file, and to move to the arbitrary Boolean expression capabilities of FIPS 201 when it is found that the fixed set of Boolean combinations offered by GSC-ISv2.1 and CAC is not sufficient to represent a required data security policy.

Migration Strategy for Key Management

One of the impediments to building general-purpose GSC-ISv2.1 BSI applications and interoperable card management systems is the lack of compatibility across applications with respect to key management information. FIPS 201 addresses this issue by providing the cryptographic information application.

The FIPS 201 cryptographic information application provides standardized method to represent, store and retrieve descriptions of all of the authentication and cryptographic capabilities of the card and the applications installed on the card. It does not, of course, provide access to key material. Thus, for example, the cryptographic information application would indicate that the card was capable of such-and-such a biometric

authentication protocol and that it contained the private key that went with such-and-such public key certificate.

Part of the migration to FIPS 201 is the movement of key management information out of the individual applications and into the cryptographic information application. The key material itself – the PKI objects, the biometric templates, the PINs, the DES keys, the RSA private keys, etc. – as well as the encoding of this key material remains the purview of individual applications and is only handled by the applications responsible for them. What is coordinated and represented in a common way is the description of the authentication and cryptographic capabilities of the applications.

Migration of the Card Edge

A fundamental difference between the GSC-ISv2.1 card edge and FIPS 201 card edge is that the card commands defined in GSC-ISv2.1 are regarded as virtual card commands that can be mapped to the commands actually implemented on the card. The card edge commands in FIPS 201 appear at the real card edge and thus no mapping is necessary.

While GSC-ISv2.1 provided for command mapping, by and large little mapping was actually done in real implementations and in particular none was done for the three GSC-ISv2.1 card applications. Furthermore, since card management and administration was not covered in GSC-ISv2.1 only proprietary card edge commands where used here and these were never mapped either.

FIPS 201 defines specific card edge commands for the management and administration of both application software and application data on the card. It leaves unchanged the card edge commands of the three GSC-ISv2.1 applications which, as noted above, non-virtual card edge commands on today's cards.

Card Edge Commands for Data Management

Tables 7-9 list the card edge commands that are provided at the card edge for data mangement by each of the three specifications under discussion.

FIPS 201 Draft	*GSC-ISv2.1*	*CAC*
	GET RESPONSE	
READ BINARY	READ BINARY[1]	
UPDATE BINARY	UPDATE BINARY[1]	
GET DATA	READ BUFFER[1]	READ BUFFER
PUT DATA	UPDATE BUFFER[1]	UPDATE BUFFER
	SELECT DF[1]	
	SELECT EF UNDER SELECTED DF[1]	
SELECT FILE	SELECT FILE[1]	
	SELECT MASTER FILE (Root) [1]	
SELECT APPLICATION	SELECT APPLET[1]	

	SELECT OBJECT[1]	
GET DATA	GET PROPERTIES[1]	GET PROPERTIES[3]
GET DATA	GET ACR[1]	

Table 7: Card Edge Commands for Data Management

FIPS 201 Draft	*GSC-ISv2.1*	*CAC*
EXTERNAL AUTHENTICATE	EXTERNAL AUTHENTICATE[2]	EXTERNAL AUTHENTICATE[3]
GET CHALLENGE	GET CHALLENGE[2]	GET CHALLENGE[3]
INTERNAL AUTHENTICATE	INTERNAL AUTHENTICATE[2]	
VERIFY	VERIFY[2]	PIN VERIFY[3]
CHANGE REFERENCE DATA	N/A	CHANGE PIN / UNBLOCK
RESET RETRY COUNTER	N/A	
		ACTIVCARD EXTERNAL AUTHENTICATE
		UPDATE / CHANGE PIN AFTER FIRST USE

Table 8: Card Edge Commands for Identification

FIPS 201 Draft	*GSC-ISv2.1*	*CAC*
MANAGE SECURITY ENVIRONMENT	MANAGE SECURITY ENVIRONMENT[1]	
PERFORM SECURITY OPERATION	PERFORM SECURITY OPERATION[1]	
	PRIVATE SIGN/DECRYPT[1]	PRIVATE SIGN/DECRYPT
READ BINARY/GET DATA		GET CERTIFICATE

Table 9: Card Edge Commands for Private Key Operations

Card Edge Commands for Application Management

Table 10 lists the card edge commands that are provided at the card edge for card management by each of the three specifications under discussion

FIPS 201 Draft	*GSC-ISv2.1*	*CAC*
CREATE FILE	N/A	
DELETE FILE	N/A	
CARD CONTENT MANAGEMENT REQUEST	N/A	INSTALL

LOAD	N/A	
DELETE APPLICATION	N/A	
GENERATE ASYMMETRIC KEY PAIR	N/A	GENERATE KEY
		INITIALIZE UPDATE[3]
		PUT KEY[3]

Table 10: Card Edge Commands for Card Management

Migration Strategy for Card Edge Interoperability

As noted in the overview, both virtual machine cards and file system cards provide means to add new card edge commands after the cards are in the field.

Virtual machine cards would need to add an applet that supports the new commands. This applies no matter what the new commands are.

Providing the card is capable of the functionality of the new command, a file system card need only have its card capability container updated with a mapping for the new commands.

Migration Strategy for On-Card Data Sharing

FIPS 201 provides an additional model for sharing data between on-card applications over and above the model for data sharing provided by the VM part of the GSC-ISv2.1 specification and the CAC specification.

The model of data sharing found in the GSC-ISv2.1 and CAC specifications is a explicit application-to-application model where one application knows by fixed application identifier which other application holds the data it is to use and the application holding the data knows by fixed application identifier which other applications can access its data.

The additional model of data sharing found in FIPS 201 is a database model where the data is held in a repository outside of any task-specific application. Applications are granted privileges to access specific items in the repository and thus share data implicitly by having overlapping data access privileges.

If the number of data items being shared among on-card applications is small and relatively static and if the pattern of sharing is primarily one application to another, then the application-to-application model of data sharing found in the GSC-ISv2.1 and CAC specifications is sufficient. If however the number of shared data items is expected to grow over time or if there are data items that all applications – existing ones and any new ones added to the card – are expected to share then the application-to-application model breaks down and the database model is more economical to manage and easier to use.

The on-card data sharing capabilities specified in FIPS 201 include the existing application-to-application model data sharing capabilities so if this model of on-card data sharing is satisfactory, no migration strategy for on-card data sharing need be contemplated.

If the database model of data sharing is more appropriate for a particular card program than the application-to-application model, then new cards can be introduced into the program that implement the new model without affecting the usage of cards in the program using the old model since the technique used to share data among on-card applications is transparent to card use applications. Of course, the program's card management applications would have to be able to support both models.

The database model of data sharing can be introduced into virtual machine cards either by providing a data repository applet or by providing an application programming interface to a file system. Both approaches are found in existing card programs.

Conclusion

FIPS 201 separates the functionality of card management and administration from the functionality of individual card applications. The standard covers the management and administration of both application software and application data through out their lifecycle on the card, from initial loading onto the card, through in-use updating and to final deletion from the card.

FIPS 201 provides a sufficiently detailed technical description of the card management and administration protocols and procedures that independent implementations of FIPS 201 card management and administration systems are themselves interchangeable and create cards that are interoperable.

FIPS 201 also standardizes the interface to three specific card applications: a generic data storage application, a symmetric key application and a public key application. These three card application were defined in GSC-ISv2.1 and the definitions provided there are preserved in FIPS 201. Technical details have been added so that like card management and administration, independent implementations are interchangeable and interoperable.